REMARKS

Claims 1–22 and 40 are pending in the present application. Claims 7–9 and 13–15 are withdrawn. Claims 1, 16, and 40 are in independent form. Claims 2–6 and 10–12 depend from independent claims 1, while claims 17-22 depend from claim 16. In the aforementioned final Office Action, claims 1–6, 10–12, 16–22 and 40 were examined and rejected. In view of the above amendments and following remarks, Applicant respectfully requests reconsideration of the Application.

Amendments to the Claims

Independent claims 1, 16, and 40 have been amended to better distinguish the term "secured file." No new matter is added by way of these amendments.

Rejections under 35 U.S.C. § 102(e) per Medoff

In paragraph 3 of the final Office Action, the Examiner rejected claims 1–6, 10–12, 16–22 and 40 under 35 U.S.C. § 102(e) as being anticipated by Medoff (Pub. No. US 2003/0088517, hereinafter *Medoff*). The Applicant respectfully traverses the Examiner's 35 U.S.C. § 102(e) rejection, because *Medoff* does not contain each and every element of these claims.

Claim 1 recites, in part, "determining whether the source file is a secured file, where the secured file cannot be accessed without *a priori* knowledge." In exemplary embodiments, a 'secured file' is a file or document that has data that cannot be accessed without *a priori* knowledge. One example of the *a priori* knowledge is a password. Another example of the *a priori* knowledge is a file key available only to an authenticated user. (See *Application* [0017]).

A close reading of the cited portions of *Medoff* disclose methods to prevent copying and printing of web pages. These web pages are not secured files, where

the secured file cannot be accessed without *a priori* knowledge. In fact, these web pages are not files as described and claimed in the present Application. The web pages merely contain private offering information which may be protected from being copied or printed. As such, there cannot be any determination of whether the source file is a secure file, since the web page is not a source file.

Claim 1 further recites "preventing subsequent usage of the designated content in a destination application via the clipboard application when said determining determines that the source file is a secured file." As such, a clipboard application prevents the usage of the designated content.

Medoff discloses a server that "transmit(s) a message to the client device instructing it to limit unauthorized use, such as copying and printing of the private offering information. In particular, the message includes an instruction to the client device to open a second browser window that does not have any printing features." (See *Medoff* [0012]). Furthermore, the message may include "an instruction to the client device to disable key functions of keyboard and mouse devices to limit printing and copying of the private offering information." (See *Medoff* [0012]). As such, it is not the clipboard application that prevents subsequent usage of the designated content, but a server that authorizes access to the private offering information.

As each and every claim element of claim 1 is not taught by *Medoff*, claim 1 is not anticipated by *Medoff*. Claims 2–6 and 10–12 depend from independent claim 1. As such claims 2-6 and 10-12 are not anticipated for at least the same reasons as claim 1.

With respect to claim 16, the element of "determining whether the source file is a secured file, where the secured file cannot be accessed without *a priori*

knowledge" is present. As previously discussed, *Medoff* does not disclose this element.

Furthermore, claim 16 recites, "preventing storage of the designated content to the clipboard application when said determining determines that the source file is a secured file." As *Medoff* does not disclose a clipboard application, as discussed above with respect to claim 1, *Medoff* cannot prevent storage of the designated content to the clipboard application."

Even if the Examiner contends that the clipboard application is a part of the server, the argument would not lend itself to claim 16. It is nonsensical to contend that *Medoff* prevents storage of the designated content to the server when said determining determines that the source file is a secured file. As such, claim 16 is not anticipated by *Medoff*. Because claims 17-22 depend from claim 16, these claims are not anticipated by *Medoff* for at least the same reasons as claim 16.

Claim 40 has similar limitations as those of claim 1. Specifically, claim 40 determines "whether the source file is a secured file, where the secured file cannot be accessed without *a priori* knowledge" and prevents "subsequent usage of the designated content in a destination application via the clipboard application when said determining determines that the source file is a secured file." Therefore, claim 40 is not anticipated for at least the same reasons as claim 1.

Rejections under 35 U.S.C. § 102(b) per Mast

In paragraph 4 of the final Office Action, the Examiner rejected claims 1–6, 10–12, 16–22 and 40 under 35 U.S.C. § 102(b) as being anticipated by Mast (U.S. Patent No. 5,881,287, hereinafter *Mast*). Applicant respectfully traverses the

Examiner's 35 U.S.C. § 102(b) rejection, because *Mast* does not contain each and every element of these claims.

Claim 1 recites, in part, "determining whether the source file is a secured file, where the secured file cannot be accessed without *a priori* knowledge" and "preventing subsequent usage of the designated content in a destination application via the clipboard application when said determining determines that the source file is a secured file." A close reading of *Mast* indicates that *Mast* does not teach determining whether a source file is a secured file and preventing subsequent usage based on this determination, but "identifying whether the image data therein is to be protected." (col. 3, line 33). Thus, *Mast* is not concerned with the security of the file, but of images deciphered and loaded into the video adapter memory. (See *Mast*, Abstract).

In fact, *Mast* states that encryption of the files (one example of file security) is not necessary for the present invention to function. (col. 7, lines 42-43). The focus of *Mast* is the prevention of the unlicensed transfer of image data within a file. Thus, the prevention of the usage of the content (i.e., the images) is not based on whether the file, itself, is secured, but whether the image data in the file is protected.

As each and every claim element of claim 1 is not taught by *Mast*, claim 1 is not anticipated by *Mast*. Claims 2–6 and 10-12 depend from independent claim 1. As such these claims are not anticipated for at least the same reasons as for claim 1.

Claim 16 also recites the limitation of "determining whether the source file is a secured file, where the secured file cannot be accessed without *a priori* knowledge." Additionally, claim 16 recites "preventing storage of the designated content to the clipboard application when said determining determines that the source file is a secured file."

As discussed above with respect to claim 1, *Mast* does not prevent usage, and thus storage, of the designated content when said determining determines that the source file is a secured file. Instead, *Mast* bases the prevention of usage on whether the image data in a file is protected, regardless of whether the file itself is secured/protected. As such, claim 16 is not anticipated by *Mast* for at least this reason.

Claims 17-22 depend from claim 16. Therefore, claims 17-22 are not anticipated for at least the same reasons as claim 16.

Claim 40 also recites the limitations of "determining whether the source file is a secured file, where the secured file cannot be accessed without *a priori* knowledge" and "preventing subsequent usage of the designated content in a destination application via the clipboard application when said determining determines that the source file is a secured file." Therefore, claim 40 is not anticipated for at least the same reasons as claim 1.

Rejections under 35 U.S.C. § 102(a) per SecurityOptions

In paragraph 5, the Examiner rejected claims 1–6, 10–12, 16–22 and 40 under 35 U.S.C. § 102(a) as being anticipated by SecurityOptions, [hereinafter *SecurityOptions*]. Applicant respectfully traverses.

As discussed above, independent claims 1, 16, and 20 recite, in part, "determining whether the source file is a secured file, where the secured file cannot be accessed without *a priori* knowledge." One example of the *a priori* knowledge is a password. Another example of the *a priori* knowledge is a file key available only to an authenticated user. (See *Application* [0017]).

SecurityOptions does not teach determining whether a source file is a secured file, where the secured file cannot be accessed without *a priori* knowledge. Instead, the files are assigned indicating elements prior to distribution. These indicating elements are not *a prior* knowledge.

Specifically, *SecurityOptions* discloses,

> The SecurityOptions element specifies settings for securing the content of a document. iSiloX and iSiloXC add indicators to the converted document so that conforming applications that utilize the document can determine what types of actions to allow on the document. [*Page 1*].

Although *SecurityOptions* teaches methods to prevent copying documents, *the* methods used to prevent copying are not based on *a priori* knowledge. The documents are associated with indicating elements whereby the elements are specific to the allowed functions, (e.g., CopyAndPaste specifies that copying to the clipboard should be allowed"). This is contrary to determining whether the source file is a secured file as is claimed in claim 1. As such, claim 1 is not anticipated by *SecurityOptions*.

Claims 2–6 and 10–12 depend from independent claim 1. As such these claims are not anticipated for at least the same reasons as claim 1 discussed above.

Independent claims 16 and 40 have the similar element of "determining whether the source file is a secured file, where the secured file cannot be accessed without *a priori* knowledge." As such claims 16 and 40 are not anticipated for at least the same reasons as claim 1. Claims 17–22 depend from independent claim 16. Therefore, these claims are not anticipated for at least the same reasons as claim 16.

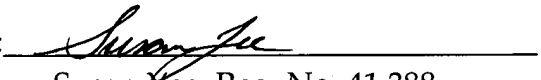
Conclusion

Based on the above remarks, Applicant believes that the rejections in the final *Office Action* are fully overcome, and that the Application is in condition for allowance. Applicant respectfully requests the passage of the present application to issue. If the Examiner has any questions regarding the present application or other issues that might be expedited through a telephone conference rather than a written action, the Examiner is invited to contact the Applicant's undersigned representative at the number provided below.

Respectfully submitted,

Patrick Zuili

Date: November 15, 2006

By: 

Susan Yee, Reg. No. 41,388
Carr & Ferrell LLP
2200 Geng Road
Palo Alto, CA 94303
Phone: (650) 812-3400
Fax: (650) 812-3444